REMARKS

This amendment is submitted in response to the Office Action dated December 29, 2006. Reconsideration and allowance of the claims is requested. In the Office Action, claims 1-27 are rejected under 35 USC §101 as not reciting a tangible or useful result. Therefore, the claims have been appropriately amended to clearly establish that a fragmented packet is received and reassembled prior to transfer to a firewall device, the packet then being transferred to the firewall device for application of firewall policies. This is clearly a useful and tangible result.

Claim 2 is rejected under 35 USC §112 as being indefinite. The claim has been amended to eliminate this issue.

Claims 1-5,10-13 and 17-27 are rejected under 35 USC §103(a) as unpatentable over Internet Protocol (RFC 791; DARPA Internet Program Protocol Specification; September 1981) (hereinafter RFC) in view of Malagrino, et al. (US 6,714,985). Claims 6-9 and 14-17 are further rejected over RFC and Malagrino in view of Mogul, et al. (Path MTU Discovery, RFC 1191, November 1990). These rejections are respectfully traversed.

According to the prior art (of which the stated RFC article is an example), IPv4 has header structures that support the fragmentation of packets. This is done to allow a router to immediately forward packets in cases where the packets are too large to fit within the required outgoing interface. Network systems, however, impose no requirement that fragments of the packets will arrive in order or that they will all arrive.

In such implementations, fragmentation causes fragments to be dropped. In fact, this is what would occur in the cited RFC article, as the cited pages make clear that the input buffer is of limited size and may be expected to be overwritten. Further, the fragmentation disclosed in the cited RFC specification is subject to more than one type of failure, as described in the present application. For example, a packet may be sent that is more than 65,535 bites in length. When reassembled, the packet overwrites the packet reassembly buffer in the host which can be no more than 65,535 bites long, causing a crash. The system described in the references may also be subjected to an attack where a fragment is used as a wedge to open a hole in the firewall to which anything may be sent. In firewalls of the type described in the Malagrino patent, fragments are treated relatively loosely by keeping track of the IP address pairs between which traffic has previously been transmitted. An attack can be made by sending a small fragment consisting of only a TCP header through the firewall. After doing this, the firewall would allow any traffic between the indicated IP addresses, regardless of which TCP port was used for transmitting any subsequent packets. In other stateless firewalls, fragmentation is handled by simply dropping fragments.

In the present invention, now described in detail in the amended claims, fragments are set aside, and reassembly buffers in the firewall with appropriate indexing are utilized to keep track of the incoming fragments and to assure their proper assignment to the reassembled packet. Specifically, the connection tables and the NAT, cited in claim 1 and 11, enable such tracking and indexing.

Once all fragments have arrived, the packet is reassembled and thereafter subject to the firewall inspection. Subsequent reassembly requires minimal states at the IP layer and avoids complicating the state machine for statefull inspection at the expense of a small amount of memory used for the reassembly buffers. The memory is reclaimed every time a packet is successfully reassembled or when the reassembly time has expired flushing the temporary buffer. The reassembled packet is then inspected in the firewall using the exact inspection logic on an unfragmented packet. Neither reference described the application of firewall policies to fully reconstituted packets at one time as claimed in every claim in the present application.

The claimed approach handles the normal case of fragmented packets in which fragments may arrive out-of-order. Such out-of-order arrival may be evidence of an attack on the firewall or maybe just that the writing order changed while the fragmented packet was on its way to the firewall.

Therefore, the claimed approach, which all independent claims clearly recite, is conducted before firewall inspection of the incoming packet and after reassembly of the received fragmented packet, is clearly different than that cited in either reference. The RFC reference clearly teaches a different approach to both identifying and handling incoming packets than claimed herein. The Malagrino reference is conceded by the Examiner to teach a different approach reassembling a packet and does not teach the claimed method of identifying packets, sorting packets and assembling them on a buffer prior to firewalling which is applied to the entire reassembled packet at one time. The Mogul reference also does not teach the claimed features of identifying and indexing patents or hashing them to make use of the index tables all conducted in a simple low memory usage state machine prior to application of firewall principles.

In view of these clear distinctions, reconsideration and allowance of claims is respectfully requested.

Respectfully submitted,

James A Sheridan

James A. Sheridan
Registration No. 25,435
PATTERSON & SHERIDAN, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846
Attorney for Applicant(s)